

## CLAIMS

1. A method, comprising:  
encoding a public key in one or more ink strands;  
embedding the one or more ink strands in a printing material; and  
5 wherein the public key is uniquely associated with an electronic  
signature that is unique to a user.
2. The method as recited in claim 1, further comprising deriving the  
public key from information associated with the user.
- 10 3. The method as recited in claim 1, wherein the printing material  
further comprises ink.
4. The method as recited in claim 1, further comprising:  
15 assigning a private key to the user; and  
deriving the public key using the private key.
5. The method as recited in claim 1, further comprising:  
receiving a password from the user; and  
20 deriving the public key using the password.
6. The method as recited in claim 1, further comprising placing the  
printing material including the ink strands into a writing instrument.

7. The method as recited in claim 1, further comprising placing the printing material including the ink into a replaceable cartridge for a writing instrument.

8. The method as recited in claim 1, further comprising distributing the printing material including the ink strands to the user.

9. The method as recited in claim 1, wherein the ink strands further comprise microscopic particles that contain public key data.

10. The method as recited in claim 1, wherein the ink strands further comprise deoxyribonucleic acid (DNA) strands that are arranged in such a way as to denote the public key.

11. One or more computer-readable media containing computer-executable instructions that, when executed on a computer, perform the following steps:

receiving an electronic document that has been converted from a paper document having a physical signature;

detecting one or more ink strands in ink used to create the physical signature;

identifying a public key denoted by one or more of the one or more ink strands;

locating an electronic signature uniquely associated with the public key;

and

attaching the electronic signature to the electronic document to create an electronically signed electronic document.

12. The one or more computer-readable media as recited in claim 11,  
5 wherein the identifying a public key further comprises reading a public key from one or more of the one or more ink strands, the public key being stored on each of the one or more ink strands.

13. The one or more computer-readable media as recited in claim 11,  
10 wherein the identifying a public key further comprises determining the public key from a coded arrangement of a plurality of the one or more ink strands.

14. The one or more computer-readable media as recited in claim 11,  
wherein the identifying a public key further comprises determining the public  
15 key from a unique arrangement of deoxyribonucleic acid (DNA) strands that are included in the one or more ink strands.

15. The one or more computer-readable media as recited in claim 11,  
wherein the locating an electronic signature further comprises:  
20 accessing an electronic signature database that contains a plurality of electronic signatures and a plurality of public keys, each electronic signature being uniquely associated with one or the plurality of public keys;  
finding a public key in the electronic signature database that matches the public key identified by the ink strands; and

if the public key identified in the ink strands is found in the electronic signature database, locating the electronic signature that is uniquely associated with the public key found in the electronic signature database.

5           16.    The one or more computer-readable media as recited in claim 15, further comprising retrieving the located electronic signature from the electronic signature database.

10           17.    A method for converting a physical signature to an electronic signature, comprising:  
              identifying a public key from one or more ink strands contained in ink in which the physical signature was created;  
              locating the public key in an electronic signature database;  
              identifying an electronic signature in the electronic signature database  
15   that is uniquely associated with the public key; and  
              substituting the electronic signature in place of the physical signature.

20           18.    The method as recited in claim 17, wherein the identifying a public key further comprises reading the public key from one or more of the one or more ink strands.

25           19.    The method as recited in claim 17, wherein the identifying a public key further comprises decoding a public key from a specific arrangement of a plurality of the one or more ink strands.

20. The method as recited in claim 17, wherein the locating further comprises accessing an electronic signature authority to access the electronic signature database.

21. The method as recited in claim 17, wherein the substituting further comprises attaching the electronic signature to an electronic document that is an electronic version of a paper document to which the physical signature was affixed.

22. An electronic signature database stored on one or more computer-readable media, comprising:

a plurality of electronic signatures, each electronic signature being uniquely associated with a user;

a plurality of public keys, each public key being uniquely associated with one of the electronic signatures; and

wherein an electronic signature for a particular user can be identified by locating a public key that is associated with the particular user.

23. The electronic signature database as recited in claim 22, wherein each public key in the database is incorporated into ink strands embedded in ink contained in a writing instrument under the exclusive control of the user.

24. A system, comprising:

an electronic signature database for storing a plurality of electronic signatures and a plurality of public keys, each electronic signature being

uniquely associated with a user and each public key being uniquely associated with an electronic signature;

a public key module configured to create the public keys from data associated with each user uniquely associated with each public key; and

5 an embedding module configured to program a public key from the electronic signature database into one or more ink strands.

25. The system as recited in claim 24, wherein the embedding module is further configured to embed the ink strands into ink.

26. The system as recited in claim 24, further comprising:

a user interface configured to accept a password from a user;

a password module configured to prompt the user via the user interface for a password that is private to the user, and to accept a private password from  
15 the user; and

wherein the password accepted from the user is used to derive the public key uniquely associated with the user.

27. The system as recited in claim 24, wherein the ink strands are  
20 embedded in ink to create signed ink, and further comprising means to securely transfer the signed ink to the user so that the signed ink is under the exclusive control of the user.

28. The system as recited in claim 24, further comprising a private  
25 key module configured to assign a unique private key to a user, wherein the

private key for a user is used at least in part to create the public key assigned to the user.

09967051-092801  
T08260-15079660